



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/735,087	12/11/2000	David Michael Kum	20206-033 (P00-3017)	5325

7590 07/13/2004  
Hewlett-Packard Company  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

EXAMINER

SON, LINH L D

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 07/13/2004

10

Please find below and/or attached an Office communication concerning this application or proceeding.

2

**Office Action Summary**

Application No.

09/735,087

Applicant(s)

KURN ET AL.

Examiner

Linh LD Son

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 11 December 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 13 and 14 recites the limitation "the sensitive information" in claim 1.

There is insufficient antecedent basis for this limitation in the claims. Appropriate correction is necessary.

Claim 28 and 29 recites the limitation "the sensitive information" in claim 16.

There is insufficient antecedent basis for this limitation in the claims. Appropriate correction is necessary.

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

1. Claims 1-29 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The language of the claim raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a

Art Unit: 2135

practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

2. Claims 1, and 16 claimed a cryptographic system do not require a program or software to carry out the task. It is an abstract idea. Further, the claimed language is not tangibly embodied. The disclosed cryptographic system in claims 1 and 16 does not include program code operating on a medium or hardware.
3. Claims 9-11, 13, and 24-26 claimed two or more master keys are kept in non-swappable physical memory, and virtual memory. The claim of the data storing in a medium is directed to non-statutory subject matter, because it is a non-functional descriptive material claiming.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. **Claims 1-6, 9-21, and 24-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al (US/6044155).**

Art Unit: 2135

6. As per claims 1 and 16, Thomlinson et al disclose the "Method and System for Securely archiving core data secrets" invention which include a cryptographic system, comprising: at least one process; two or more master keys (Figure 3) of which at least one master key is a most-secure master key and requiring a multi-part construction to be exposed (Master Key, Col 11 lines 44-53), relative to the at least one most-secure master key each of the remaining one or more master keys is a less-secure master key and requiring construction from fewer parts to be exposed (Item Key, Col 13 lines 20-25). Thomlinson et al teach the implementation of the Message Authentication Code (MAC) to create a linking mechanism between keys for verification (Col 11 lines 15-20). Further, Thomlinson et al do teach a linking means between the item and the item authentication key to detect any tampering done to the item key (Col 11 lines 30-44) using the (MAC). However, Thomlinson et al do not teach specifically the linking means of the *most-secure master key (Master key)* and the *less secure master key (Item key)*. Therefore, it is obvious at the time of the invention was made for one of ordinary skill in the art to implement the same link means using the (MAC) to the most secure master key (Master key) and the less secure master key (item key) to detect any tampering done to the less-secure mater keys (item key).
7. As per claims 2 and 17, the same basis rejection of claim 1 applies. Further, store the MAC in the computer (Col 11 lines 54-60).

8. As per claims 3, 4 18, and 19, Thomlinson et al disclose a cryptographic system as in claims 1, 3, and 16, wherein the cryptographic linking is performed by creating a message digest of the one or more most-secure master keys concatenated with a random value and further concatenated with the one or more less-secure master keys, and saving the result in a database (Col 11 lines 30-44, and Col 55-60). Same rejection basis is applied from claim 1. Further, the random value is a salt is obvious at the time the invention was made for one of ordinary skill in the art (Col 11 line 51).
9. As per claims 5 and 20, Thomlinson et al a cryptographic system as in claim 1. However, Thomlinson et al do not specifically use most-secure master key as a symmetric encryption key directly, to compute a symmetric message authentication code, and retaining some or all of the result. Nevertheless, Thomlinson et al do teach the use of the symmetric encryption algorithm (Col 4 lines 37-40), and the generating and encrypting method of the MAC using item authentication key, which is encrypted using the Master key (Col 11 line 60 to Col 12 line 5). The chain of encryption described in Col 11 line 60 to Col 12 line 5 will further protecting the MAC which the applicant claimed invention's main purpose. Therefore, it is obvious at the time of the invention was made for one of ordinary skill in the art to use the most secure master to encrypt the MAC.

Art Unit: 2135

10. As per claims 6 and 21, Thomlinson et al disclose a cryptographic system as in claims 1 and 16 and the cryptographic linking (See basis of rejection in claim 5). However, Thomlinson et al do not teach the symmetric message authentication code (MAC) is an 8-byte data size, and retaining a 4-byte portion of the result. Nevertheless, Thomlinson et al specify the implementation of the DES encryption method (Col 4 line 50) in the invention. Therefore, it is obvious at the time of the invention was made for one of ordinary skill in the art to produce the 8-byte data size (64 bits) and the retaining a 4-byte (32 bits) portion of the result is to increase the security of the MAC and also to reduce the data storage volume.
11. As per claims 9-11, and 24-26, Thomlinson et al disclose a cryptographic system as in claims 1, 9, 16, and 23, wherein the two or more master keys are kept in non-swappable physical protected memory (Col 11 lines 54-59) and in the virtual memory (Col 6 line 3).
12. As per claims 12 and 27, a cryptographic system as in claims 1 and 16, wherein, respectively, the at least one most-secure master key and the one or more less-secure master keys, including a protection key (Master Key) and an integrity key protecting access to sensitive information and the integrity key (item keys) ensuring the integrity of the sensitive information (Col 11 line 60 to Col 12 line 5).

Art Unit: 2135

13. As per claims 13 and 28, Thomlinson et al disclose a cryptographic system as in claims 1 and 16, wherein the sensitive information is kept in a database (Col 4 lines 23-26).
14. As per claims 14 and 29, Thomlinson et al disclose a cryptographic system as in claims 1 and 16, wherein the sensitive information can be a public key (Col 1 lines 12-15, and Col 4 lines 23-26).
15. As per claim 15, a cryptographic system as in claims 1 and 16, wherein the means for cryptographically linking is a key repository process for enforcing enterprise policies and policy decisions (Col 1 lines 12-15).
16. **Claims 7-8, and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomlinson et al in view of Matyas et al (US/4941176).**
17. As per claims 7 and 22, Thomlinson et al disclose a cryptographic system as in claims 6 and 16. However, Thomlinson et al do not teach the use of Cipher-block chaining (CBC) method to compute the symmetric message authentication code. Nevertheless, Matyas et al do implement the CBC in the "Secure Management of Keys using Control Vectors" invention (Col 45 lines 8-17). Therefore, it is obvious at the time the invention was made for one of ordinary



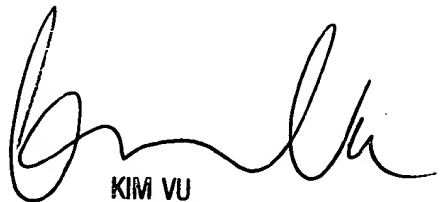
skill in the art to use the same algorithm operation to ensure the data correction for the MAC.

18. As per claims 8 and 23, Thomlinson et al and Matyas et al disclose a cryptographic system as in claims 7 and 16, wherein the CBC is performed using a random number as an initialization vector, and wherein the initialization vector is saved along with the result (Matyas et al, Col 125 line 18).

## Conclusion

1. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (703)-305-8914 or Fax to 703-746-9821.
2. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (703)-305-4393. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (703)-305-9600.

Linh LD Son  
Patent Examiner

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100